



TITLE:

GFSR法による生成列の重み分布の偏りについて(確率数値解析に於ける諸問題,II)

AUTHOR(S):

栗田, 良春; 松本, 眞

CITATION:

栗田, 良春 ...[et al]. GFSR法による生成列の重み分布の偏りについて(確率数値解析に於ける諸問題,II). 数理解析研究所講究録 1995, 932: 82-102

ISSUE DATE:

1995-12

URL:

<http://hdl.handle.net/2433/59973>

RIGHT:

GFSR法による生成列の重み分布の偏りについて*

栗田 良春[†](KURITA Yoshiharu[†]) 松本 眞[§](MATSUMOTO Makoto[¶])

平成7年 11月 3日

要旨

m -系列から構成される GFSR (Generalized Feedback Shift Register) 列が 0,1 の出現順序に関して偏りを持つことを連続した部分列の重みの平均的な推移を表す伝達関数を導入して示す. 特に, 原始3項式による m -系列では, この偏りが大きい. この解析から, その欠陥への parameter の依存性について明らかにし, GFSR 法のための原始多項式の選択指針を示す. この指針による, 最適な原始5項式の探索を行い結果を例示する.

1 GFSR (Generalized Feedback Shift Register) 法

2 値 0,1 をとる系列 $\{a_0, a_1, \dots\}$ が次の2つの条件を満たす時, この列を最大周期列 (maximum-length linear feedback shift register sequence, 略して m -系列) という.

(i) 次の p 次の線型漸化式に従う列である: $a_i = h_1 a_{i-1} + h_2 a_{i-2} + \dots + h_p a_{i-p} \pmod{2}$,
ここに $h_p = 1$, h_k は 0 または 1 ($1 \leq k \leq p-1$), $i = p, p+1, \dots$.

(ii) 初期値 a_0, a_1, \dots, a_{p-1} をすべて 0 ではないように与えた時, 周期は最大値 $2^p - 1$ である.

2 値系列 $\{a_i\}$ が m -系列であるための条件は (i) に示した漸化式の特性多項式 $x^p + h_{p-1}x^{p-1} + \dots + 1$ が GF(2) 上の原始多項式であることである.

GFSR 法とは, 上の漸化式で a_i を word 長の vector として生成した vector 列を擬似一様乱数として使用するものである. 従って, その各 bit は同じ漸化式を満たす m -系列となり, 最上位 bit についても例外でないことに注意したい.

2 三項漸化式の非乱数性

m -系列は擬似乱数としての周期全体にわたるいくつかの望ましい性質をもつ. 特に Golomb[2] によって指摘された randomness の次の3つの要請, すなわち, (a) 0 と 1 の個数の balance, (b) 連の長さの分布, (c) two-leveled auto-correlation, を満たしている. 上述のように, 2 値 m -系列は

*Deviation of Weight Distribution of GFSR-sequences

[†]計量研究所, 〒305 つくば市梅園1-1-4, e-mail kuri @nrlm.go.jp

[‡]National Research Laboratory of Metrology

[§]慶応義塾大学理工学部数理科学科, 〒223 横浜市港北区日吉3-14-1, e-mail matumoto@math.keio.ac.jp

[¶]Dept. Math. Yagami, Keio Univ.

GF(2)上の原始多項式を特性多項式として生成されるが、その生成効率の観点から項数が最少である原始3項式を用いて、Lewis and Payne [6]によって実際的な生成algorithmが提案された。この方法はTLP法とも呼ばれ、乗算型線形合同式法の本質的な欠陥（超格子構造をもつこと）の指摘もあって、その優位性が注目され、広く使われていると思われる。

このTLP法は、しかしながら統計的検定に関する著者達の実験では、ほとんど常にrejectされる。それは、後でより正確に述べることにするが、「原始3項式による m -系列では0の個数が期待値よりも多すぎる部分列があり、1についてはそうではない」と要約される非対称の性質を持ち、TLP列のmost significant bitにこの性質が直接に反映するという事実による。この報告の目的は、2つのtuple間の重みの推移を、すなわち部分列の性質を、重み伝達関数の導入によって解析し、その欠陥をより明確にするものである。

以下、具体的に述べる。

$$\{a_i\} = a_0, a_1, a_2, \dots, a_{N-1} \quad (1)$$

を0または1の値をとる周期 N の m -系列とし、

$$g(X) = X^p + X^q + 1, \quad (2)$$

ここに $p > 2q^1$ 、を列(1)のGF(2)上の特性多項式（原始3項式）とする²。このとき、 m -系列(1)は $P = 2^p - 1$ の周期を持ち、つぎの漸化式をみたす：

$$a_{n+p} + a_{n+q} + a_n = 0 \pmod{2}. \quad (3)$$

次に、 $A_{n,M}$ を(1)の第 n 項から始まる M -tupleとする： $A_{n,M} = \{a_n, a_{n+1}, \dots, a_{n+M-1}\}$ 、そして $w(A_{n,M})$ をこの M -tupleのweight、すなわち1の個数とする： $\sum_{k=0}^{M-1} a_{n+k}$ 、ここに添字 $n+k$ は周期を法としてとることとする。

さて、この m -系列が真の2値乱数列であるとする、次の2つの性質(p1)と(p2)をもつことが期待される。

(p1) W を M -tupleの重みを表す確率変数とすると、 W の確率密度関数は次の二項分布に従う：

$$Prob(W = k) = B_{M,1/2} = \binom{M}{k} \left(\frac{1}{2}\right)^M. \quad (4)$$

ここに、 $\binom{M}{k}$ は二項係数、 $1 \leq k \leq M$ 。

(p2) 互いに素な任意の2つの M -tupleの重みは統計的に独立である。

次の定理は重みの分布に関して情報を与える：

[定理A]（例えば、Golomb[2], pp.43-44を参照）周期 $2^p - 1$ の任意の m -系列において、長さ M のbit patternの1周期における出現回数は、すべて0のpatternについては $2^{p-M} - 1$ 、そうでないpatternについては 2^{p-M} である、ここに $1 \leq M \leq p$ 。

¹ $q > p/2$ の場合を考える必要はない：(2)の相反3項式 $X^p \cdot g(1/X)$ は再び原始的であって、この2つは順序が逆で同じ列を生成する。

² 実用上の目的からここでは p は $89 \leq p \leq 1279$ の範囲のMersenne指数とする（Zierler[7], Bright and Enison[1]を参照）

この定理で述べているのは、しかしながら、 $M \leq p$ の場合の出現回数についてだけであって、その出現順序についてではない。そして事実、上にのべた (p2) は成立していないことが次のような方法で簡単に確かめられる： $M \geq p$ に対して列 (1) から N 個の引き続いた、互いに素な M -tuples: $A_{0,M}, A_{M,M}, \dots, A_{(N-1)M,M}$ を取り出す。こうして得られる重み分布のヒストグラムと期待分布 (4) を比較することにより、系統的偏りがほとんどいつでも検出できる。そこでは観測した実測分布の殆どは 2 項分布に比べて一般的に、「左の尾が長く、左肩は痩せ、右肩は太り、右尾はない」形をもち、skewness を表わす 3 次 moment は負である³。言葉を換えれば、隣り合う 2 つの p -tuple の遷移が uniform でないということになる。

3 p -tuple の重みの推移における平均的振舞いの解析

ここでは、重み伝達関数を導入し、それを用いて $M = p$ の場合の前節でのべた偏りを解析する。

[定理 B] $f(r)$ を $w(A_{n,p}) = r$ であるときの $w(A_{n+p,p})$ の平均値とする。ここに、 $r \in [1:p]$ 。このとき、

$$f(r) = \frac{r}{(p-1)(p-2)} \{4\lambda r^2 - 2((1+2\lambda)p - 2(1-\lambda))r + (2+\lambda)p^2 - (4-\lambda)p + 2\lambda\}, \quad (5)$$

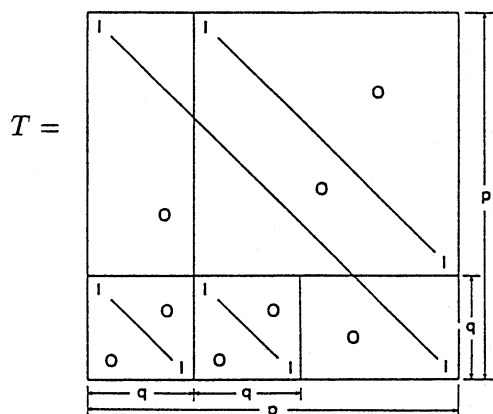
ここに、 $\lambda = q/p$ ($0 < \lambda < 1/2$)。

[証明] 次節定理 C の証明に含まれるので省略する。ただし、この場合の遷移行列 T を掲げておく：

p -tuple $A_{n,p}$ を列ベクトルとする。漸化式 (3) から、次式が成立する。

$$A_{n+p,p} = T \cdot A_{n,p} \bmod 2, \quad (6)$$

ここに、 T は次の形をもつ $(p \times p)$ 行列である。



4 原始 t 項式 ($t \geq 3$) への weight transfer function の導入

$[GF(2)]^p$ 上の 2 つの vector を考える：

³ この偏りは tuple の長さ $M = \alpha \cdot p$, ($1 < \alpha < \sim 20$) でいつでも観測される。

$$\mathbf{t} = (t_0, t_1, \dots, t_{p-1}), \quad \mathbf{x} = (x_0, x_1, \dots, x_{p-1}).$$

ここに各要素はすべて0または1. この内積 $\mathbf{t} \cdot \mathbf{x}$ を次のように定義する:

$$\mathbf{t} \cdot \mathbf{x} = \sum_{i=0}^{p-1} t_i x_i \pmod{2}.$$

また, vector \mathbf{a} の重み (要素中の1の個数) を $w(\mathbf{a})$ で表す. このとき, 次の定理がなりたつ.

[定理C] ([3] 参照) $w(\mathbf{t}) = \nu$, $w(\mathbf{x}) = r$, $1 \leq \nu \leq p$, $1 \leq r \leq p$ とし, \mathbf{x} は, その weight が r であるようなすべての bit pattern を平等に確からしくとる random vector とする. この時, 内積 $\mathbf{t} \cdot \mathbf{x}$ の期待値 $E(\mathbf{t} \cdot \mathbf{x})$ は次のように求められる⁴.

$$\begin{aligned} E(\mathbf{t} \cdot \mathbf{x}) &= \frac{1}{\prod_{k=0}^{\nu-1} (p-k)} \sum_{l=1,3,5,\dots,\leq \nu} \binom{\nu}{l} \left\{ \prod_{k=0}^{l-1} (r-k) \right\} \left\{ \prod_{k=0}^{\nu-l-1} (p-r-k) \right\} \\ &= \frac{1}{\binom{p}{r}} \sum_{l=1,3,5,\dots,\leq \nu} \binom{p-\nu}{r-l} \binom{\nu}{l}. \end{aligned}$$

但し, 積記号 $\prod_{k=0}^*$ において, $* < 0$ の場合には, この積の値は1とする.

[証明1] $w(\mathbf{x}) = r$ であって, x のどの要素についても, その要素が1である確率は r/p であることに注意する. はじめに, $\nu = 2, 3$ の場合について考え, それを一般化する.

i) $\nu = 2$ の場合.

\mathbf{t} の要素のうち, 1である要素を t_{i_1}, t_{i_2} とする.

x_{i_1} または x_{i_2} のどちらかだけが1である確率は $\binom{2}{1} \frac{r}{p} \cdot \frac{p-r}{p-1}$. これが $E(\mathbf{t} \cdot \mathbf{x})$ である.

ii) $\nu = 3$ の場合.

\mathbf{t} の要素のうち, 1である要素を $t_{i_1}, t_{i_2}, t_{i_3}$ とする.

$x_{i_1}, x_{i_2}, x_{i_3}$ のうち, ひとつだけが1である確率は $\binom{3}{1} \frac{r}{p} \frac{p-r}{p-1} \frac{p-r-1}{p-2}$.

$x_{i_1}, x_{i_2}, x_{i_3}$ の3つが共に1である確率は $\binom{3}{3} \frac{r}{p} \frac{r-1}{p-1} \frac{r-2}{p-2}$. これらの和が $E(\mathbf{t} \cdot \mathbf{x})$ である.

iii) $\nu = \nu$ の場合について, 次のように書き下すことができる: \mathbf{t} の要素のうち, 1である要素を $t_{i_1}, t_{i_2}, \dots, t_{i_\nu}$ とする.

$x_{i_1}, x_{i_2}, \dots, x_{i_\nu}$ のうち, どれかひとつだけ1である確率は

$$\binom{\nu}{1} \frac{r}{p} \frac{p-r}{p-1} \frac{p-r-1}{p-2} \dots \frac{p-r-(\nu-2)}{p-(\nu-1)}.$$

$x_{i_1}, x_{i_2}, \dots, x_{i_\nu}$ のうち, 3つだけ1である確率は

⁴ここで, 二項係数 $\binom{n}{k}$ は一般的な規約に従うものとする. すなわち $n < k$ または $k < 0$ の時 $\binom{n}{k} = 0$, 但し $n > 0$.

$$\binom{\nu}{3} \frac{r}{p} \frac{r-1}{p-1} \frac{r-2}{p-2} \frac{p-r}{p-3} \frac{p-r-1}{p-4} \cdots \frac{p-r-(\nu-4)}{p-(\nu-1)}.$$

こうして,

$x_{i_1}, x_{i_2}, \dots, x_{i_\nu}$ のうち l ($\text{odd}, \leq \nu$) 個だけ 1 である確率は

$$\begin{aligned} & \binom{\nu}{l} \cdot \frac{r}{p} \frac{r-1}{p-1} \cdots \frac{r-(l-1)}{p-(l-1)} \frac{p-r}{p-l} \frac{p-r-1}{p-l-1} \cdots \frac{p-r-(\nu-l-1)}{p-(\nu-1)} \\ &= \binom{\nu}{l} \frac{1}{\prod_{k=0}^{\nu-1} (p-k)} \prod_{k=0}^{l-1} (r-k) \prod_{k=0}^{\nu-l-1} (p-r-k). \end{aligned}$$

$E(\mathbf{t} \cdot \mathbf{x})$ は上式の $l = 1, 3, 5, \dots \leq \nu$ についての総和である.

(証明終)

[別証] \mathbf{t} の要素のうち, 1 である要素を $t_{i_1}, t_{i_2}, \dots, t_{i_\nu}$ とする.

これらの ν 個の bit のうちから, 1 を入れるべき l 個の bit を選び出す場合の数は $\binom{\nu}{l}$. 但し, $l \leq \nu$. $(p-\nu)$ 個の bit のうちから, $(r-l)$ 個ある残りの 1 を入れるべき $r-l$ 個の bit を選び出す場合の数は $\binom{p-\nu}{r-l}$. パタンの総数は, p 個の bit のうちから, 1 を入れるべき r 個の bit を選び出す場合の数 $\binom{p}{r}$ に等しい. こうして定理の第 2 式を得る.

(証明終)

さて, ここで $E(\mathbf{t} \cdot \mathbf{x})$ を (p を fix した時の) r, ν の関数として考え,

$$h_p(r, \nu) = E(\mathbf{t} \cdot \mathbf{x})$$

とする. このとき, 次の補題が成り立つ:

[補題 1] p, r, ν を正整数, $1 \leq \nu \leq p, 1 \leq r \leq p$ であれば, $h_p(r, \nu) = h_p(\nu, r)$.

[証明] 次式が成立する;

$$h_p(r, \nu) = \frac{1}{p!} \sum_{l=1,3,5,\dots \leq \nu} \frac{\nu(\nu-1) \cdots (\nu-l+1) \cdot r(r-1) \cdots (r-l+1) \cdot (p-\nu)!(p-r)!}{(p-r-\nu+l)! l!}.$$

これから, \sum の右側は ν, r について対称であることが分かる. さて $\nu = r$ の時は明らか. $\nu < r$ と仮定すると

$$\begin{aligned} h_p(r, \nu) - h_p(\nu, r) &= \sum_{l=1,3,5,\dots \leq \nu} \{\cdots\} - \sum_{l=1,3,5,\dots \leq r} \{\cdots\} \\ &= - \sum_{\nu < l \leq r, l: \text{odd}} \{\cdots\}. \end{aligned}$$

$\{\cdots\}$ について次式が成立する.

- (1) $(p-\nu)! \geq 0, (p-r)! \geq 0$.
 (2) $\nu(\nu-1)\cdots(\nu-l+1)$ については $\nu-l < 0$ から $\nu-l+1 < 1$. 従って $\nu(\nu-1)\cdots(\nu-l+1) = 0$.
 (3) $(p-r-\nu+l)!$ については $\nu-l < 0$ から $p-r-(\nu-l) > p-r > 0$.
 従って $(p-r-\nu+l)! > 0$.

こうして $\sum_{\nu < l \leq r, l: \text{odd}} \{\cdots\} = 0$. $\nu > r$ の時も全く同様に証明できる.

(証明終)

$h_p(r, \nu)$ では, r は 1 から p までの整数値をとるが, 以後しばらくの間, 関数の振舞いを調べるため, r は同範囲の連続値をとるものとしよう. 更に, 定義域, 値域ともに $(-1/2, 1/2)$ とするために, 次のように $h_p(r, \nu)$ を再定義する:

$$y_p(x, \nu) = h_p\left(\left(x + \frac{1}{2}\right)p, \nu\right) - \frac{1}{2}.$$

すなわち,

$$y_p(x, \nu) = \frac{1}{\prod_{k=0}^{\nu-1} (p-k)} \left[\sum_{l=1,3,5,\dots,\nu} \binom{\nu}{l} \prod_{k=0}^{l-1} \left\{ \left(\frac{1}{2} + x\right)p - k \right\} \prod_{k=0}^{\nu-l-1} \left\{ \left(\frac{1}{2} - x\right)p - k \right\} \right] - \frac{1}{2}.$$

この時, 次の補題が成立する.

[補題 2] $y_p(x, \nu)$ は, 偶関数 (ν : even の時), または奇関数 (ν : odd の時) である.

[証明] 次式が成立することに注意する (その証明はたとえば Knuth[4], p58.):

$$\sum_{l=0,1,2,\dots,\nu} \binom{p-r}{\nu-l} \binom{r}{l} = \binom{p}{\nu}. \quad (7)$$

$z_p(x, \nu) = y_p(x, \nu) + 1/2$ とおく. 更に $\nu-l = l'$ とおくと,

$$\binom{\nu}{l} = \binom{\nu}{l'}, \quad \prod_{k=0}^{l-1} = \prod_{k=0}^{\nu-l'-1}, \quad \prod_{k=0}^{\nu-l-1} = \prod_{k=0}^{l'-1}$$

であるから, 次の (i), (ii) が成立する:

- (i) ν : even の時, $l = 1, 3, 5, \dots, \nu-1$ に対応して $l' = \nu-1, \nu-3, \dots, 1$.
 故に $z_p(-x, \nu) = z_p(x, \nu)$, すなわち $y_p(-x, \nu) = y_p(x, \nu)$.
 (ii) ν : odd の時, $l = 1, 3, 5, \dots, \nu$ に対応して $l' = \nu-1, \nu-3, \dots, 0$.

こうして,

$$z_p(x, \nu) + z_p(-x, \nu) = \frac{1}{\prod_{k=0}^{\nu-1} (p-k)} \sum_{l=1,2,3,\dots,\nu} \binom{\nu}{l} \prod_{k=0}^{l-1} \left\{ \left(\frac{1}{2} + x\right)p - k \right\} \prod_{k=0}^{\nu-l-1} \left\{ \left(\frac{1}{2} - x\right)p - k \right\}$$

$$= 1$$

が成立する. 何故ならば, 右辺は ν 次の多項式, 従って異なる $\nu+1$ 個の x に対して1であれば, これは恒等的に1となる. ところで等式(7)から, $-1/2 \leq x \leq 1/2$ に対応する r ($0 \leq r/p \leq 1$)のうちから $p+1$ 個の異なる値: $r = 0, 1, 2, \dots, p$ を選ぶことができて補題が成立. 更に, $p+1 \geq \nu+1$ であるから証明できた.

(証明終)

さて, 関数 $y_p(x, \nu)$ がどのような関数であるかを具体的に知ることが重要であるが, 次のような簡潔な漸化式がなりたつ.

[定理D] 任意の $0 < p, \nu$ と任意の x に対して, 次の漸化式が成り立つ.

$$y_p(x, \nu+1) + \frac{2px}{p-\nu} \cdot y_p(x, \nu) + \frac{\nu}{p-\nu} \cdot y_p(x, \nu-1) = 0,$$

$$y_p(x, 1) = x, \quad y_p(x, 0) = 1/2.$$

[証明] y_p の定義にもどり, 漸化式を h_p で書き直すと,

$$(p-\nu)h_p(r, \nu+1) + (2r-p)h_p(r, \nu) + \nu h_p(r, \nu-1) = r$$

と同値であることがわかる. さて,

$$h_p(r, \nu) = \frac{1}{\binom{p}{r}} \sum_{l=1,3,5,\dots,\leq \nu} \binom{p-\nu}{r-l} \binom{\nu}{l}.$$

であったが, ここで, $\binom{\nu}{l}$ などを ν の多項式と見て実関数に拡張すると, $0 \leq \nu < l$ なる整数では0をとるようになる. これに注意すると, 添字 l は $0 \leq l \leq p$ なる奇数を全て走るとしてもよい. (以後単に $l: \text{odd}$ と書く.)

上式の両辺を $\binom{p}{r}$ 倍したものを証明する.

$\binom{\nu+1}{l} = \frac{\nu+1}{\nu-l+1} \binom{\nu}{l}$ の公式を使えば, 左辺の三項は全て $F_{p,r,\nu,l} := \binom{p-\nu}{r-l} \binom{\nu}{l}$ の一次結合で表される. すなわち, 左辺の三つの項の和は

$$\sum_{l:\text{odd}} F_{p,r,\nu,l} \left\{ (p-\nu) \frac{p-\nu-r+l}{p-\nu} \cdot \frac{\nu+1}{\nu-l+1} + (2r-p) + \nu \frac{p-\nu+1}{p-\nu-r+l+1} \cdot \frac{\nu-l}{\nu} \right\}$$

で表される. 一方, 右辺は

$$r \binom{p}{r} = (p-r+1) \binom{p}{r-1}$$

であるが, 公式

$$\binom{p}{r} = \sum_l \binom{p-\nu}{r-l} \binom{\nu}{l}$$

で r を $r+1$ に置き換え, l の奇偶を分けることにより

$$\begin{aligned}
(p-r+1)\binom{p}{r} &= (p-r+1) \sum_{l:\text{odd}} \left\{ \binom{p-\nu}{r-1-l} \binom{\nu}{l} + \binom{p-\nu}{r-l} \binom{\nu}{l} \right\} \\
&= (p-r+1) \sum_{l:\text{odd}} F_{p,r,\nu,l} \left\{ \frac{r-l}{p-\nu-r+l+1} + \frac{l}{\nu-l+1} \right\}
\end{aligned}$$

を得る。よって,

$$\begin{aligned}
&(p-\nu) \frac{p-\nu-r+l}{p-\nu} \cdot \frac{\nu+1}{\nu-l+1} + (2r-p) + \nu \frac{p-\nu+1}{p-\nu-r+l+1} \cdot \frac{\nu-l}{\nu} \\
&= (p-r+1) \left\{ \frac{r-l}{p-\nu-r+l+1} + \frac{l}{\nu-l+1} \right\}
\end{aligned}$$

を証明すればよい。これは $A := p-r+1$, $B := \nu-l$ とおき, p, l を消去すると「手計算」でも検証できる。

(証明終)

上の漸化式により, $h_p(x, \nu)$ および $y_p(x, \nu)$ を次々に計算できる。また, 例えば定数項が

$$y_p(0, \nu+1) = -\frac{\nu}{p-\nu} y_p(0, \nu-1)$$

を満たすことがわかる。 ν が偶数の時にはこれは0であるが, 奇数の時には決して0にならず, その絶対値の最小値は ν が $p/2$ にもっとも近い整数で達成されることがわかる (そこまでは絶対値が1つおきに単調に減少する)。また, x が十分0に近い時は, 漸化式の中央の項の寄与は小さく, 同様の計算によって ν は $p/2$ からあまり離れないところで $|y_p(x, \nu)|$ は小さくなると考えられる。

参考までに $\nu = 1, 2, 3, 4, 5, 6$ について, $h_p(r, \nu)$ を書き下せば次の通りである。

$$\begin{aligned}
h_p(r, 1) &= r/p, \\
h_p(r, 2) &= \frac{2r(p-r)}{p(p-1)}, \\
h_p(r, 3) &= \frac{r(4r^2 - 6pr + 3p^2 - 3p + 2)}{p(p-1)(p-2)}, \\
h_p(r, 4) &= \frac{4r(-2r^3 + 4pr^2 - 3p^2r + 3pr - 4r + p^3 - 3p^2 + 4p)}{p(p-1)(p-2)(p-3)}, \\
h_p(r, 5) &= \frac{r(16r^4 - 40pr^3 + 40p^2r^2 - 40pr^2 + 80r^2 - 20p^3r + 60p^2r - 120pr + 5p^4 - 30p^3 + 75p^2 - 50p + 24)}{p(p-1)(p-2)(p-3)(p-4)}, \\
h_p(r, 6) &= \frac{2r(-16r^5 + 48pr^4 - 60p^2r^3 + 60pr^3 - 160r^3 + 40p^3r^2 - 120p^2r^2 + 320pr^2 - 15p^4r + 90p^3r - 285p^2r + 210pr - 184r + 3p^5 - 30p^4 + 125p^3 - 210p^2 + 184p)}{p(p-1)(p-2)(p-3)(p-4)(p-5)}.
\end{aligned}$$

また, $\nu = 1, 2, 3, 4, 5, 6$ について, $y_p(x, \nu)$ を書き下せば次の通りである.

$$\begin{aligned}
 y_p(x, 1) &= x, \\
 y_p(x, 2) &= \frac{1 - 4px^2}{2(p-1)}, \\
 y_p(x, 3) &= \frac{x(4p^2x^2 - 3p + 2)}{(p-1)(p-2)}, \\
 y_p(x, 4) &= -\frac{16p^3x^4 - 8(3p-4)px^2 + 3p-6}{2(p-1)(p-2)(p-3)}, \\
 y_p(x, 5) &= \frac{x(16p^4x^4 - 40(p-2)p^2x^2 + 15p^2 - 50p + 24)}{(p-1)(p-2)(p-3)(p-4)}, \\
 y_p(x, 6) &= -\frac{64p^5x^6 - 80(3p-8)p^3x^4 + 4(45p^2 - 210p + 184)px^2 - 15p^2 + 90p - 120}{2(p-1)(p-2)(p-3)(p-4)(p-5)}.
 \end{aligned}$$

これら $y_p(x, \nu)$ の振舞いの実例を Fig. 4A に示す.

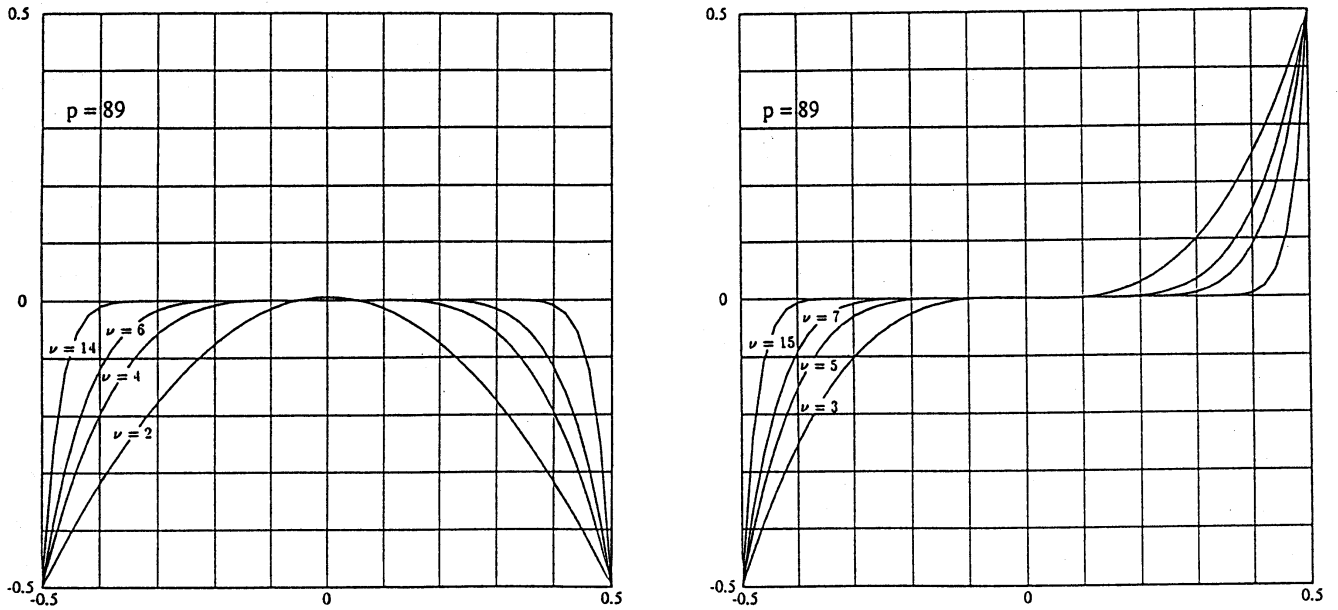


Fig. 4A Behavior of expected inner product of two random vectors on GF(2): $y_p(x, \nu)$.

この graph から視覚的に分かるが, [定理 D] の漸化式から, p, ν を定数とし, r が平均的重み $p/2$ 付近を動く変数として $h_p(r, \nu)$ を一変数関数と考えると, これは ν が $p/2$ 付近のとき定数関数 (定数 $1/2$) に近づく. したがって, 乱数性からみれば項数 ν が $p/2$ 付近になるのが望ましいといえる. 但し, 数値実験の結果から $|h_p(r, \nu) - 1/2|$ の ν についての単調性は成立しない. その数値例 ($p = 31, r = 9$) を TABLE 4A に示す.

TABLE 4A
Numerical evaluation of $h_p(r, \nu) - 1/2$

$p = 31, r = 9$			
ν	$h_p(r, \nu) - 1/2$	ν	$h_p(r, \nu) - 1/2$
0	- 0.500 00000	9	- 0.000 22859
1	- 0.209 67741	10	- 0.000 00136
2	- 0.074 19354	11	0.000 10801
3	- 0.018 79866	12	0.000 07095
4	- 0.000 77864	13	- 0.000 01966
5	0.002 41008	14	- 0.000 06545
6	0.001 35478	15	- 0.000 03385
7	0.000 12606	16	0.000 03385
8	- 0.000 32685

ここまでの用意で [定理 B] の一般化ができる. ある p -tuple \mathbf{X} (縦ベクトル) の weight を r , すなわち, $w(\mathbf{X}) = r$ ($1 \leq r \leq p$), 更に $(T_t)_{k*}$ (T の第 k 行) の weight を ν , ($0 \leq \nu \leq p$) とする. この時 $\sum_{i=1}^p (T_t)_{ki} \cdot (\mathbf{X})_i$ の weight の期待値が $h_p(r, \nu)$ である.

さて, 前節の (6) 式の推移行列 T は, 原始3項式に対するものであったから, これを T_3 と書くことにすると, T_3 についての weight transfer function: (5) 式は, 実は, $f(r) = (p-q)h_p(r, 2) + qh_p(r, 3)$ であった. すなわち, 原始3項式については, $\nu = 2$ の t が $(p-q)$ 個, $\nu = 3$ の t が q 個あって, $\nu \geq 4$ の t は存在しない. この事実由来する欠陥は既に述べたが, Fig. 4A の $\nu = 2$ の graph から, 更に (graph からは読みとり難いが) $\nu = 3$ から, 明らかとなる.

$T_t (t \geq 5)$ を, しかしながら, p, q_1, q_2, \dots によって一般式として見通しよく表現することは難しいように思われる. 具体的な原始5項式に対応する T_5 の計算結果例を Fig. 4B に示す⁵. この図において, 白丸は0, 黒丸は1を表し, T_5 の左側の3列は左から順に, 通し番号, その (通し番号の) 列の weight, その行の weight を表す. 行列右側の c 欄は histogram で, その weight をもつ列数を, 最下行の % つき数は1の占める割合を示したものである. r 欄は行についてである. 上図 (12%) と下図 (20%) を比較すると, 本章の結論から下図の行列の方が, 推移の独立性は高いことが予測される.

この2例についての weight transfer function の数値を TABLE 4B に示す. この TABLE の左側第一列は r を, 第2列は Fig. 4B の上側の遷移行列, 第3列は下側の遷移行列に対応する数値である. たとえば, 第2列について書き下せば, $p = 61$ として,

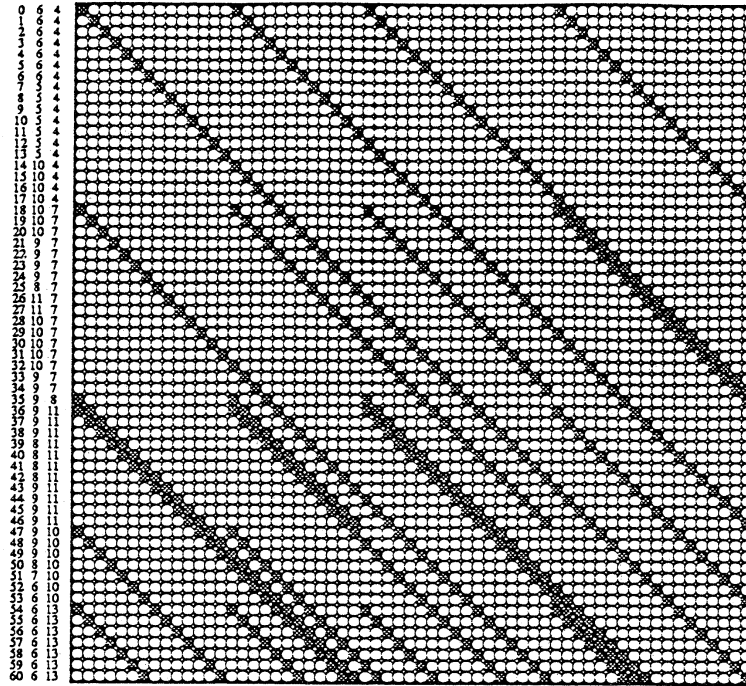
$$(18h_p(r, 4) + 17h_p(r, 7) + h_p(r, 8) + 7h_p(r, 10) + 11h_p(r, 11) + 7h_p(r, 13))/p - 1/2$$

⁵なお, 原始5項式の探索方法とその結果については Kurita and Matsumoto[5] を参照されたい.

を評価したものである。第2列, 第3列の比較から予測どおり, 第3列は約2倍第2列より精度が高く, 最も出現頻度の高い $r = p/2$ 付近では 7×10^{-5} 程度である。TABLE の右の表は比較のための, 3項式 $(x^{89} + x^{38} + 1)$ についてのものである ($p = 61$ の原始3項式は存在しない)。次数が89とより高いにも拘わらず, 偏りが極めて大きいこと (約50倍) がわかる。

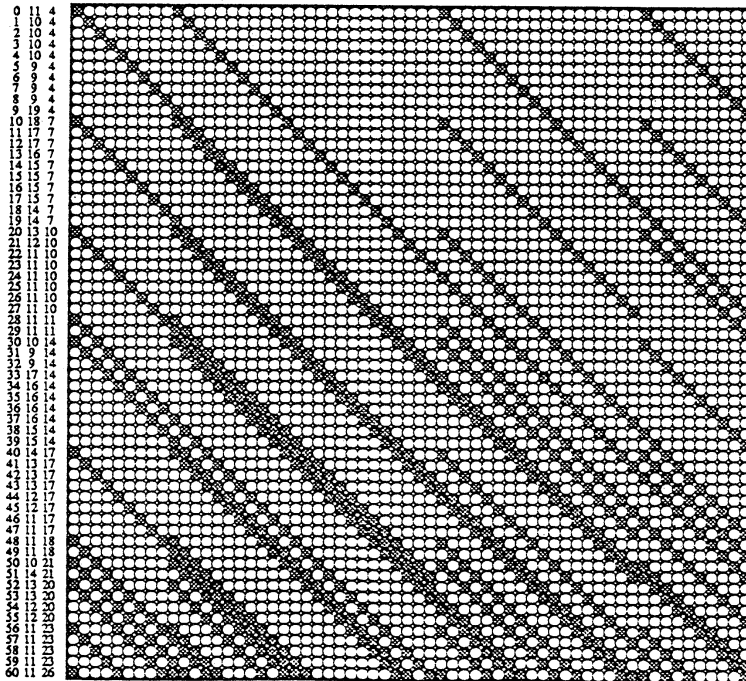
このようにして, T_t ($T \geq 5$) の各行の weight が数値として具体的に与えられた場合には p -tuple の weight の平均的推移を求めることができることになり, この尺度からの最適化をはかることが可能となった。GFSR 法のための原始多項式のひとつの選択指針がこうして得られたことになる。

c r p = 61 q1 = 43 q2 = 26 q3 = 14



c	r
5: 7	4: 18
6: 16	
7: 1	7: 17
8: 6	8: 1
9: 17	
10: 12	10: 7
11: 2	11: 11
	13: 7
12 %	12 %

c r p = 61 q1 = 51 q2 = 33 q3 = 9



c	r
	4: 10
	7: 10
9: 6	
10: 6	10: 8
11: 18	11: 2
12: 5	
13: 6	
14: 4	14: 10
15: 6	
16: 5	
17: 3	17: 8
18: 1	18: 2
19: 1	
	20: 4
	21: 2
	23: 4
	26: 1
20 %	20 %

Fig. 4B Example of transition matrix T_5 (61×61) of two primitive pentanomials: $(x^{61} + x^{43} + x^{26} + x^{14} + 1)$ and $(x^{61} + x^{51} + x^{33} + x^9 + 1)$, where \circ means 0 and \bullet means 1.

TABLE 4B Numerical evaluation of weight transfer function
corresponding to Fig. 4B and primitive trinomial ($x^{89} + x^{38} + 1$).

$x^{61} + x^{43} + x^{26} + x^{14} + 1$			$x^{61} + x^{51} + x^{33} + x^9 + 1$			$x^{89} + x^{38} + 1$			$x^{89} + x^{38} + 1$		
0	- 0.5		- 0.5			0	- 0.5	45	0.003	13657	
1	- 0.370	73367	- 0.294	67884		1	- 0.472	73071	46	0.002	68600
2	- 0.276	56543	- 0.188	99041		2	- 0.446	40828	47	0.001	96533
3	- 0.207	69293	- 0.129	55739		3	- 0.421	01765	48	0.000	98959
4	- 0.157	02494	- 0.093	05667		4	- 0.396	54380	49	- 0.000	22617
5	- 0.119	46413	- 0.068	89658		5	- 0.372	97169	50	- 0.001	66693
6	- 0.091	36656	- 0.051	96941		6	- 0.350	28627	51	- 0.003	31763
7	- 0.070	13836	- 0.039	62045		7	- 0.328	47250	52	- 0.005	16325
8	- 0.053	93757	- 0.030	35706		8	- 0.307	51535	53	- 0.007	18873
9	- 0.041	45625	- 0.023	27672		9	- 0.287	39978	54	- 0.009	37906
10	- 0.031	76284	- 0.017	79855		10	- 0.268	11075	55	- 0.011	71917
11	- 0.024	18939	- 0.013	52885		11	- 0.249	63323	56	- 0.014	19404
12	- 0.018	25186	- 0.010	18931		12	- 0.231	95216	57	- 0.016	78863
13	- 0.013	59434	- 0.007	57655		13	- 0.215	05252	58	- 0.019	48789
14	- 0.009	95044	- 0.005	53796		14	- 0.198	91926	59	- 0.022	27680
15	- 0.007	11680	- 0.003	95669		15	- 0.183	53735	60	- 0.025	14030
16	- 0.004	93497	- 0.002	74169		16	- 0.168	89174	61	- 0.028	06337
17	- 0.003	27914	- 0.001	82098		17	- 0.154	96741	62	- 0.031	03096
18	- 0.002	04767	- 0.001	13686		18	- 0.141	74930	63	- 0.034	02803
19	- 0.001	15730	- 0.000	64243		19	- 0.129	22238	64	- 0.037	03955
20	- 0.000	53899	- 0.000	29913		20	- 0.117	37162	65	- 0.040	05047
21	- 0.000	13500	- 0.000	07483		21	- 0.106	18197	66	- 0.043	04576
22	0.000	10331	0.000	05745		22	- 0.095	63839	67	- 0.046	01038
23	0.000	21717	0.000	12062		23	- 0.085	72585	68	- 0.048	92929
24	0.000	24162	0.000	13413		24	- 0.076	42930	69	- 0.051	78745
25	0.000	20644	0.000	11455		25	- 0.067	73372	70	- 0.054	56983
26	0.000	13685	0.000	07591		26	- 0.059	62405	71	- 0.057	26138
27	0.000	05394	0.000	02992		27	- 0.052	08526	72	- 0.059	84706
28	- 0.000	02506	- 0.000	01386		28	- 0.045	10232	73	- 0.062	31184
29	- 0.000	08676	- 0.000	04807		29	- 0.038	66017	74	- 0.064	64067
30	- 0.000	12164	- 0.000	06744		30	- 0.032	74379	75	- 0.066	81853
31	- 0.000	12429	- 0.000	06898		31	- 0.027	33814	76	- 0.068	83036
32	- 0.000	09362	- 0.000	05206		32	- 0.022	42817	77	- 0.070	66114
33	- 0.000	03323	- 0.000	01863		33	- 0.017	99885	78	- 0.072	29581
34	0.000	04833	0.000	02663		34	- 0.014	03514	79	- 0.073	71935
35	0.000	13739	0.000	07618		35	- 0.010	52200	80	- 0.074	91672
36	0.000	21493	0.000	11947		36	- 0.007	44439	81	- 0.075	87287
37	0.000	25675	0.000	14297		37	- 0.004	78728	82	- 0.076	57277
38	0.000	23366	0.000	13034		38	- 0.002	53561	83	- 0.077	00137
39	0.000	11201	0.000	06271		39	- 0.000	67437	84	- 0.077	14365
40	- 0.000	14550	- 0.000	08081		40	0.000	81150	85	- 0.076	98455
41	- 0.000	57886	- 0.000	32246		41	0.001	93703	86	- 0.076	50905
42	- 0.001	22934	- 0.000	68499		42	0.002	71727	87	- 0.075	70210
43	- 0.002	13792	- 0.001	19061		43	0.003	16724	88	- 0.074	54866
44	- 0.003	34346	- 0.001	85990		44	0.003	30200	89	- 0.073	03370
45	- 0.004	88052	- 0.002	71042							
46	- 0.006	77687	- 0.003	75542							
47	- 0.009	05040	- 0.005	00242							
48	- 0.011	70508	- 0.006	45234							
49	- 0.014	72538	- 0.008	09942							
50	- 0.018	06782	- 0.009	93313							
51	- 0.021	64827	- 0.011	94323							
52	- 0.025	32213	- 0.014	12996							
53	- 0.028	85392	- 0.016	52209							
54	- 0.031	87091	- 0.019	20718							
55	- 0.033	79376	- 0.022	37853							
56	- 0.033	73425	- 0.026	39912							
57	- 0.030	34730	- 0.031	86091							
58	- 0.021	62030	- 0.039	55606							
59	- 0.004	57762	- 0.050	13885							
60	0.025	12765	- 0.063	02069							
61	0.073	77049	- 0.073	77049							

この指針から原始5項式を選択した例を挙げる：第5章で述べる algorithm によって次数 p の原始5項式を探索し、それぞれの p について、得られた数百個の原始5項式から T_5 の中の1の占める割合が50%に最も近い3例ずつを TABLE 4C に示す。

TABLE 4C
Examples of optimum primitive pentanomials

p	q_3	q_2	q_1	max	mean	σ	%
61	60	22	7	39	30.39	8.39	49.83
	59	34	3	46	30.44	11.55	49.91
	60	33	18	49	30.64	10.03	50.23
89	87	38	9	65	44.37	17.07	49.85
	87	43	7	59	44.51	15.98	50.01
	88	45	29	65	44.62	12.95	50.13
107	106	43	21	76	53.44	14.06	49.94
	106	89	22	74	53.60	14.07	50.09
	105	50	29	80	53.93	21.48	50.41
127	125	86	9	95	63.46	24.47	49.97
	126	28	13	99	63.50	26.82	50.00
	126	21	18	106	63.53	32.19	50.02
521	520	125	57	431	260.07	110.52	49.92
	520	342	308	402	260.72	91.80	50.04
	520	415	293	325	260.74	67.56	50.05
607	606	44	4	563	302.99	170.46	49.92
	605	418	123	446	303.05	123.05	49.93
	606	465	127	396	303.35	81.78	49.98
1279	1278	292	274	1252	639.10	346.12	49.97
	1278	366	354	1261	639.34	350.74	49.99
	1278	804	792	1249	643.25	346.07	50.29

この表では、左4列に p, q_3, q_2, q_1 を、各行のweightの最大値(max)を第5列に、行についてのweightの平均値(mean)を第6列に、その標準偏差(σ)を第7列に、そして、最右列には、行列全体の中の1の占める割合(%)を示す。なお、予想されるように、 q_3 はこの場合 p に極めて近い。この表のはじめの6行に対応する T_5 を Fig.4C(a),(b),(c);(e),(f),(g)に、また対角的な pattern をもつ原始5項式の T_5 を Fig.4C(d)に示す。

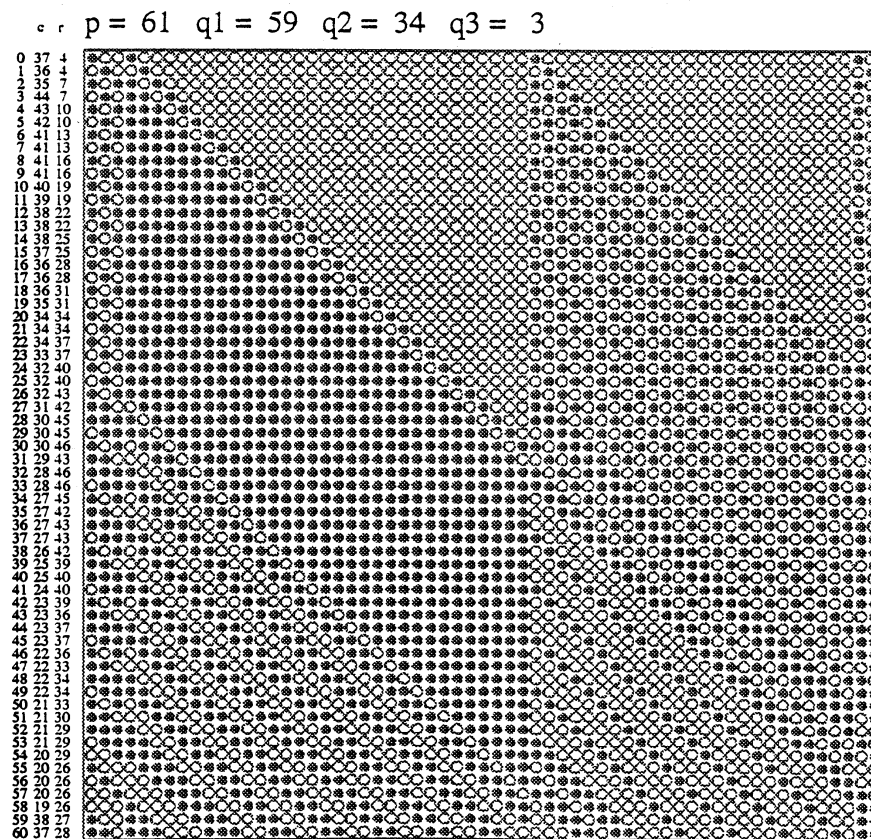
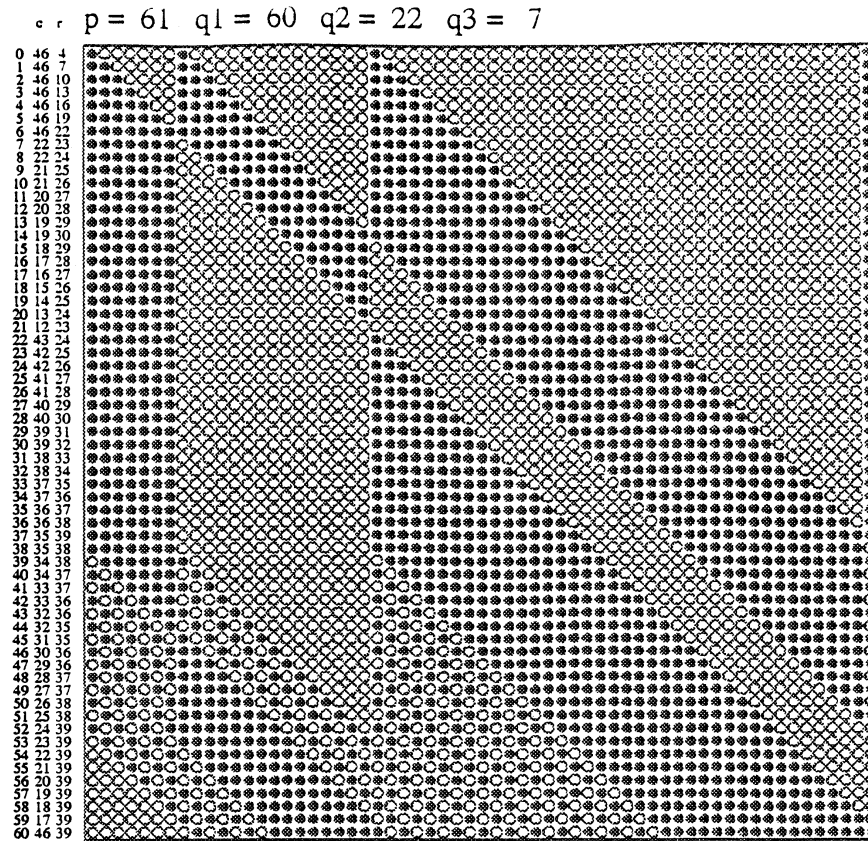


Fig. 4C(a),(b) Example of transition matrix T_5 (61×61) of two primitive pentanomials $(x^{61} + x^{60} + x^{22} + x^7 + 1)$ and $(x^{61} + x^{59} + x^{34} + x^3 + 1)$, where \circ means 0 and \bullet means 1.

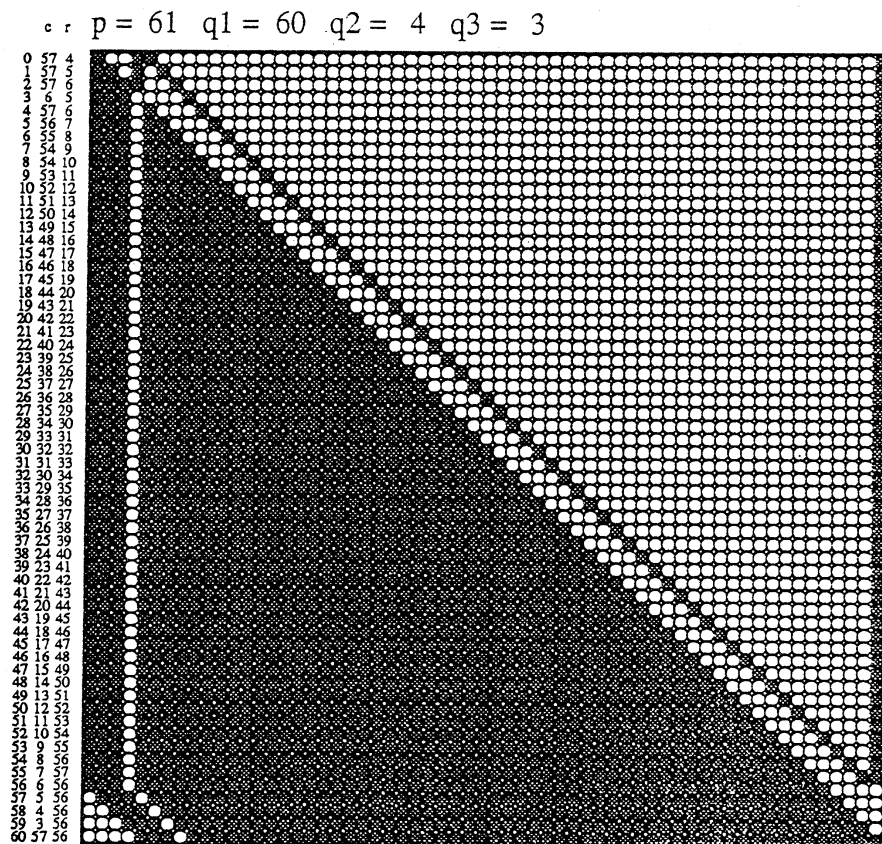
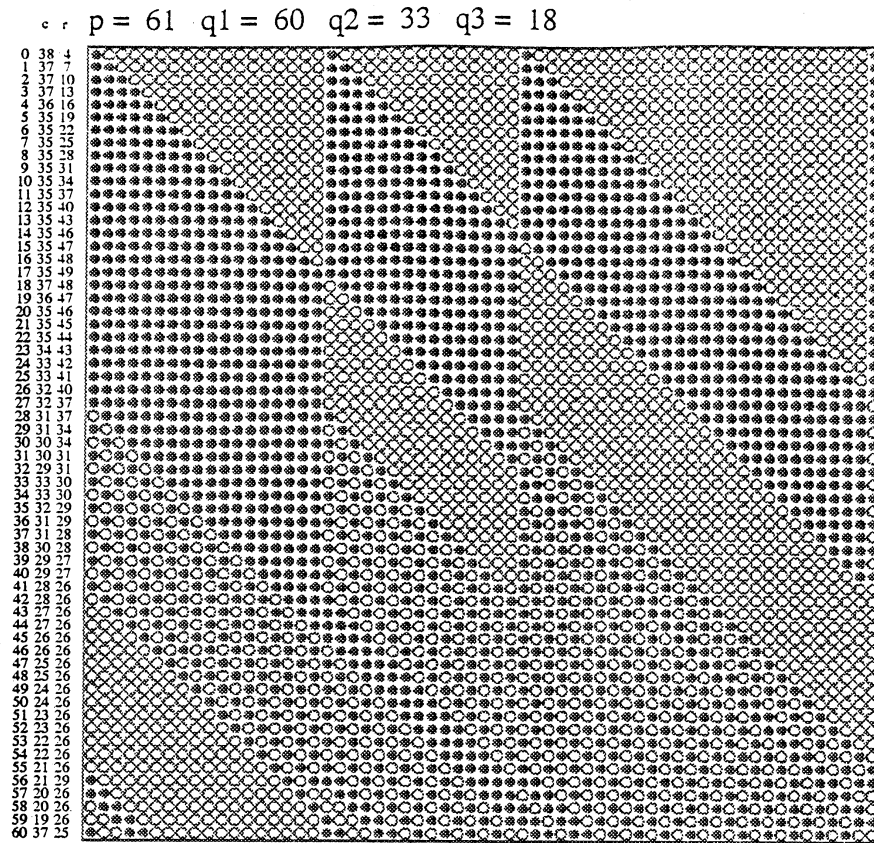


Fig. 4C(c),(d) Example of transition matrix T_5 (61×61) of two primitive pentanomials $(x^{61} + x^{60} + x^{33} + x^{18} + 1)$ and $(x^{61} + x^{60} + x^4 + x^3 + 1)$, where \circ means 0 and \bullet means 1.

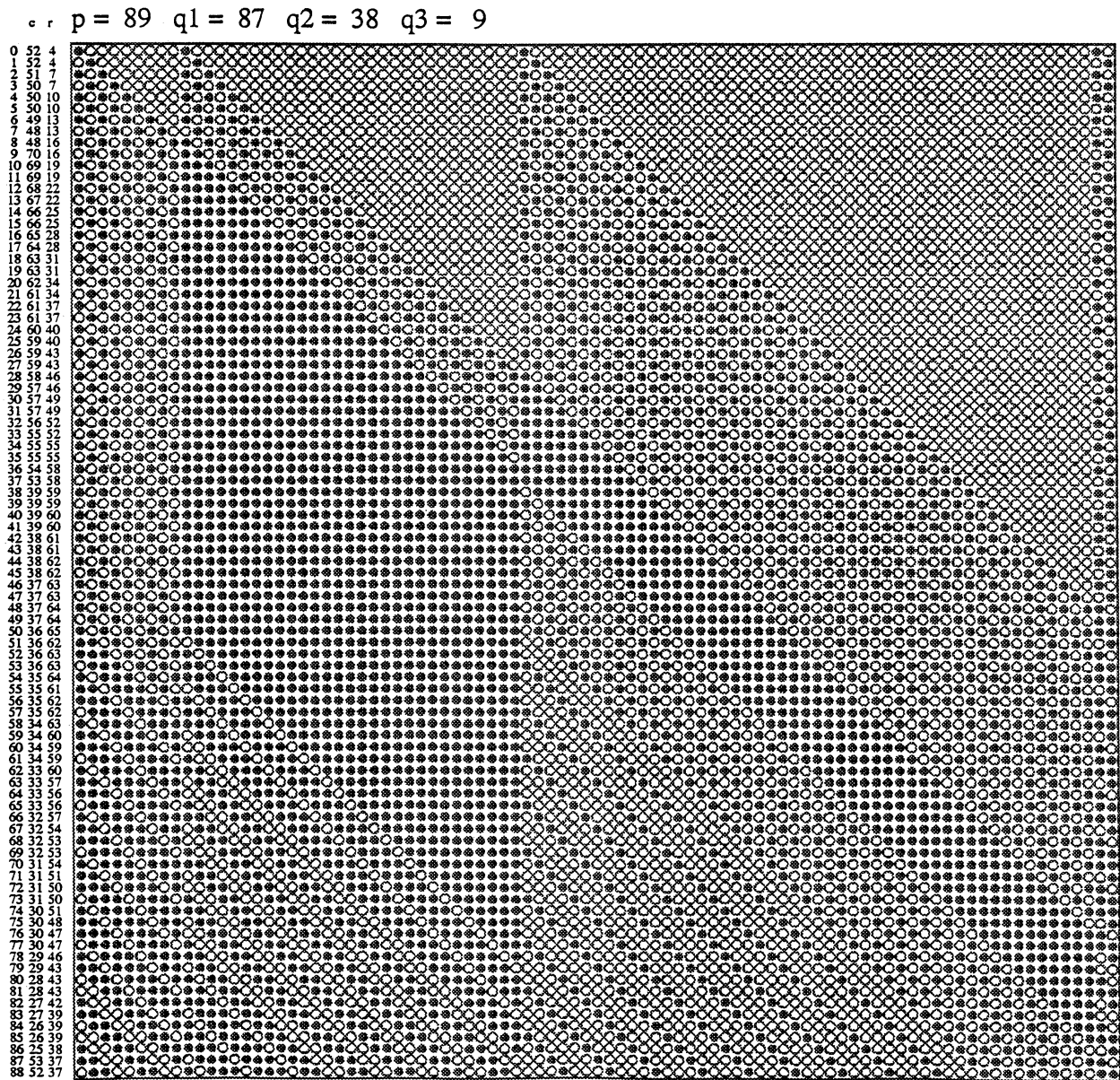


Fig. 4C(e) Example of transition matrix T_5 (89×89) of primitive pentanomial corresponding to TABLE 4C

$$(x^{89} + x^{87} + x^{38} + x^9 + 1),$$

where \circ means 0 and \bullet means 1.

c r p = 89 q1 = 87 q2 = 43 q3 = 7

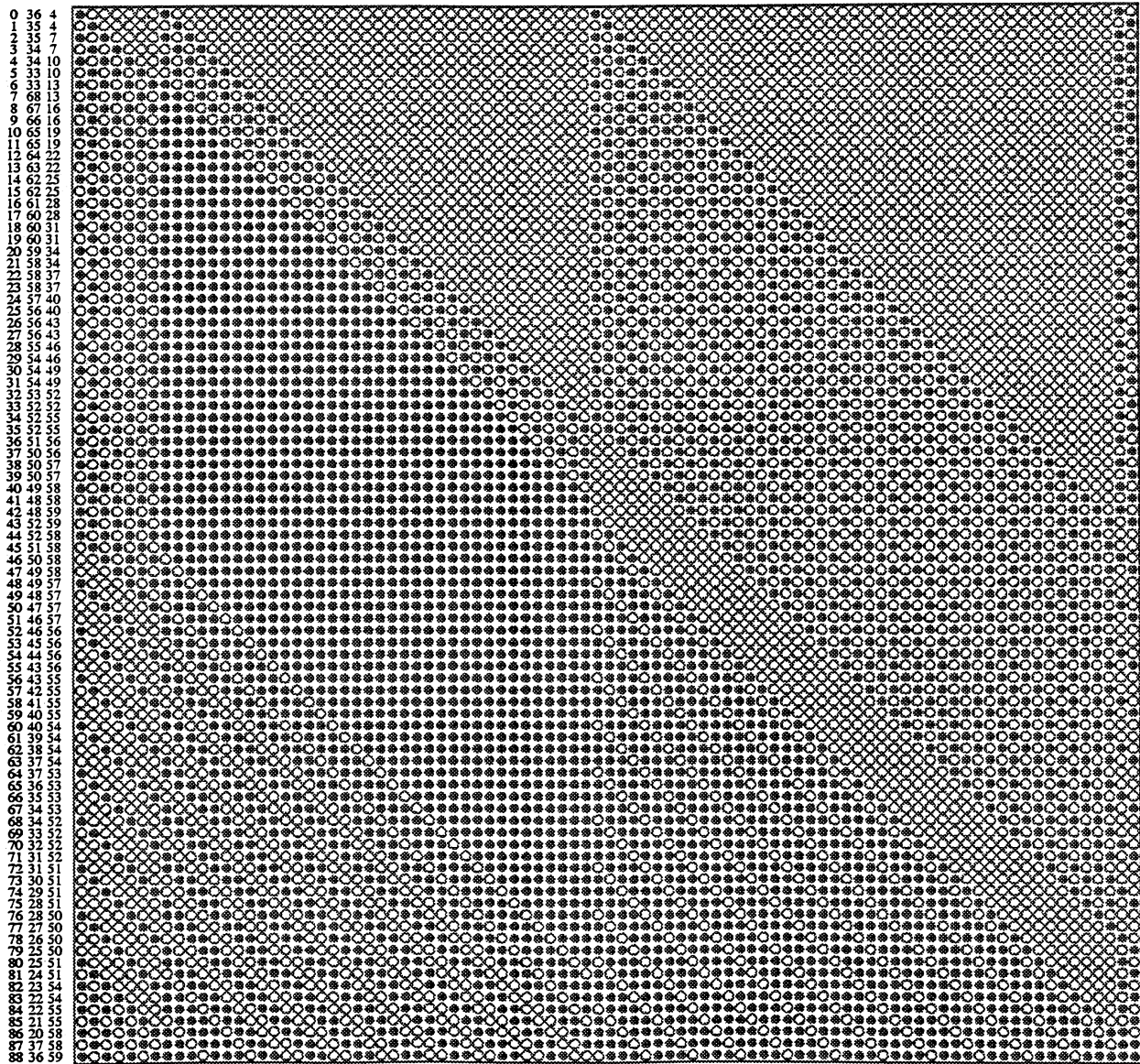


Fig. 4C(f) Example of transition matrix T_5 (89×89) of primitive pentanomial corresponding to TABLE 4C

$$(x^{89} + x^{87} + x^{43} + x^7 + 1),$$

where o means 0 and • means 1.

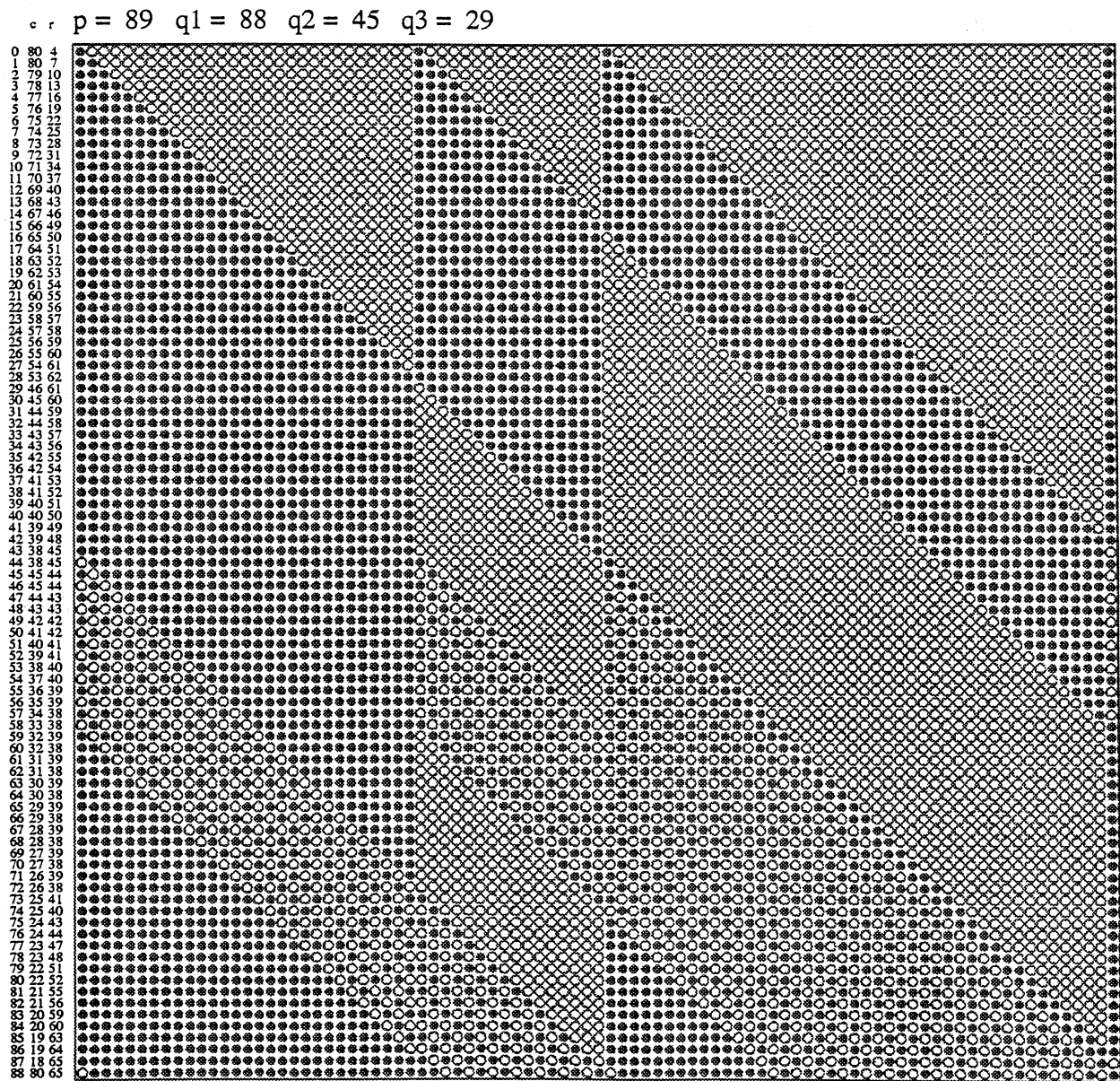


Fig. 4C(g) Example of transition matrix T_5 (89×89) of primitive pentanomial corresponding to TABLE 4C

$$(x^{89} + x^{88} + x^{45} + x^{29} + 1),$$

where \circ means 0 and \bullet means 1.

5 まとめ

主要な結果を以下に要約する：

- (i) 2値の擬似乱数列として、3項原始多項式を特性多項式とするすべての m 系列は平均として系統的な偏りをもつ。平均としての性質であるから重大な欠陥である。すなわち、引き続く重み w_k と w_{k+1} は相関を持つ。この性質により、3項 m 系列は統計的に多すぎる0を含む部分列をもち、これら過多の0がTLP列のmost significant bitに直接的に反映することになる。
- (ii) 原始3項式で、この偏りを最小にするためには、できるだけ大きい p の値を採用し、 q の値をなるべく $p/2$ に近づけることである。しかしながら、それに近い実用的な1つの組み合わせ： $p = 1279, q = 418$ の場合でも偏りは依然として検出される。
- (iii) これを避けるためには、原始 t 項式($t > 3$)を用い、その推移行列の各行のweightが $p/2$ になるべく近く、かつ、どの行も3以下でないものを選ぶ必要がある。また、奇数のweightをもつ行の数と偶数のweightをもつ行がほぼ等しいような推移行列を選ぶことも必要であろう。
- (iv) size p , weight r の random vector から ν 個成分を選んだ和(mod 2)が1となる期待値を与える関数 $h_p(r, \nu)$ の漸化式を求めた。これから、 ν が $p/2$ よりあまり離れていない時には定数関数に近いことがわかる。 T_t ($T \geq 5$)の各行のweightが数値として具体的に与えられた場合に p -tupleのweightの平均的推移を与える関数は、これらの和として書ける。この尺度からの最適化をはかることができ、GFSR法のための原始多項式のひとつの選択指針が得られた。これに基づいて最適な5項原始多項式の探索を行い結果を示した(TABLE 4C)。

参考文献

- [1] H. S. Bright and R. L. Enison. Quasi-random number sequences from a long-period tlp generator with remarks on application to cryptography. *Comput. Surv.*, 11(4):357-370, Dec. 1979.
- [2] S. W. Golomb. *Shift Register Sequences*, revised ed. Aegean Park Press, Laguna Hills, Calif., 1982.
- [3] H. F. Jordan and D. C. M. Wood. On the distribution of sums of successive bits of shift-register sequences. *IEEE Trans. Comput.*, C-22(4):400-408, Apr. 1973.
- [4] D. E. Knuth. *The Art of Computer Programming, Vol.1, Fundamental Algorithms*. Addison-Wesley, Reading, Massachusetts, 1976.
- [5] Y. Kurita and M. Matsumoto. Primitive t -nomials ($t=3,5$) over $gf(2)$ whose degree is a mersenne exponent $\leq 44\,497$. *Math. Comput.*, 56(194):817-821, Apr. 1991.
- [6] T.G. Lewis and W.H. Payne. Generalized feedback shift register pseudorandom number algorithms. *J. ACM*, 20(3):456-468, Mar 1973.

- [7] N. Zierler. Primitive trinomials whose degree is a mersenne exponent. *Inform. Contr.*, 15:67–69, 1969.